

Beneficios

Práctico y Compacto

El iKey 4000 es pequeño y de construcción resistente para seguridad extra, haciéndolo fácil de transportar lo que permite a los usuarios llevar constantemente con ellos sus identidades digitales únicas.

Conectividad USB Fácil de Desplegar

El iKey 4000 ofrece la seguridad de una smart card sin la necesidad de desplegar y mantener lectores costosos o de dispositivos biométricos costosos para aumentar sus aplicaciones de seguridad. El iKey ofrece seguridad tipo smart card sin el dolor de cabeza.

Procesamiento Criptográfico Interno

A diferencia de otras smart cards o tokens basados en sistemas de autenticación, el iKey 4000 ofrece generación de llave y procesamiento criptográfico interno para asegurar que las llaves y funciones criptográficas permanezcan seguras dentro del hardware en todo momento. De hecho, hay 64K de EEPROM disponibles para asegurar el almacenamiento de llaves, contraseñas, certificados, y datos.

Certificaciones

FIPS 140-2 Nivel 3
Common Criteria EAL 4+
RoHS
China RoHS
FCC Part 15 – Clase B
CE

SafeNet Borderless Security iKey 4000

La tecnología más avanzada en tokens USB

Construido con la tecnología criptográfica de tokens más avanzada ahora en día, el token USB iKey 4000 de SafeNet contiene 64K de EEPROM para generar y almacenar seguramente contraseñas, certificados públicos, y otros datos en un dispositivo lo suficientemente pequeño para colgarse en un llavero. Las llaves iKey 4000 aseguran que sólo los usuarios autorizados puedan realizar funciones criptográficas. El iKey 4000 se conecta a cualquier puerto USB para proveer una fuerte autenticación de usuario sin necesidad de lectores costosos.

El iKey 4000 cumple con las normas de la directiva RoHS, y es compatible con una amplia gama de aplicaciones y sistemas portátiles. Su bajo costo, diseño compacto, y su interfaz USB estándar hacen más fácil la implementación que otras opciones de tokens. Su hardware con certificación FIPS Nivel 3 (en proceso), generación interna de llave, almacenamiento de llave, encriptación, y firma digital agregan un nivel más alto de seguridad para las aplicaciones cliente.

Generación de Llave RSA/DSA

La integridad de los pares de llave pública/privada es fundamental para el éxito de cualquier sistema criptográfico. Las llaves que están almacenadas en una computadora, y sólo protegidas por software, son vulnerables a técnicas de hacking y al robo de llaves que puede pasar desapercibido. Debido a que el iKey 4000 de SafeNet desempeña todas las funciones criptográficas sensibles directamente en el token. Usuarios no autorizados no pueden de ninguna manera tener acceso a los certificados digitales de usuarios, a menos que se roben el token y adivinen el pass phrase.



El token USB líder en la industria, el iKey 4000 de SafeNet, es un token USB portátil PKI, de autenticación de dos factores que ofrece seguridad para verificación, firma, y encriptación.

Firma Digital RSA/DSS

Las funciones criptográficas que se realizan en el chip permiten a los usuarios producir firmas digitales RSA (PKCS#11) o DSS (FIPS 186) teniendo la plena seguridad de que las llaves privadas permanecerán en secreto por un largo tiempo. Sólo las llaves iKey pueden darle esta confianza duradera en los sets de llaves de firma digital.

RSA e Intercambio de Llave Diffie-Hellman

Ningún sistema está completo si no ofrece soporte para el intercambio de llave de sesión de encriptación. Los tokens iKey 4000 de SafeNet incluyen tanto key unwrapping de RSA y key agreement y funciones de intercambio de llave Diffie-Hellman. Las llaves privadas usadas en estas funciones de intercambio nunca se exponen a sistemas host vulnerables.

Seguro

El token USB iKey 4000 de SafeNet ofrece autenticación de dos factores a las aplicaciones donde la seguridad es crítica. A diferencia de la tradicional autenticación con contraseña que depende en las débiles contraseñas que se adivinan fácilmente, el iKey 4000 requiere tanto de un token físico (el iKey mismo) y el NIP del usuario para completar el proceso de autenticación. Este token de autenticación de dos factores está diseñado para todos los entornos PKI incluyendo Certificados Digitales X.509 y PGO. El almacenamiento de datos se divide en dos áreas, una en donde los certificados digitales y las llaves públicas son almacenados, y otra área para las llaves privadas y otros secretos. Solo se puede tener acceso a la llave privada por medio de autenticación y los datos se retienen en forma cifrada. El iKey 4000 es capaz de desempeñar todas las llaves privadas, públicas y funciones criptográficas secretas dentro del mismo token.

El iKey 4000 utiliza el sistema operativo del token de SafeNet y el software cliente, el cual incluye la utilidad de gestión de llave/token que se puede usar para la inicialización del token, cambio de contraseñas y etiquetas, y para el control de logging y el rastreo (tracing) de la información

Flexible

SafeNet trabaja con proveedores de software y hardware para asegurar que el iKey 4000 ofrezca la gama más amplia de soporte para soluciones de seguridad. El soporte para el iKey se incluye en Single Sign-On login, autenticación VPN, cifrado de e-mail, firmas digitales, y muchas otras aplicaciones con capacidad PKI de marcas líderes como Microsoft, Entrust, Computer Associates, VeriSign y más. El iKey 4000 es compatible con PKCS #11, Microsoft CryptoAPI, Microsoft PC/SC, y Apple Native PC/SC para una integración fácil en aplicaciones personalizadas.

Conveniente

El pequeño tamaño y construcción resistente del token iKey 4000, lo hacen fácil de transportar lo que permite a los usuarios llevar constantemente con ellos sus identidades digitales únicas. El iKey 4000 es un token compacto de autenticación de dos factores que proporciona seguridad cliente para autenticación en red, cifrado de e-mail, y aplicaciones de firma digital.

Especificaciones

Sistemas Operativos

Compatibles:

- Microsoft Windows 2000
- Microsoft Windows 2003
- Microsoft Windows XP
- Microsoft Windows Vista
- Apple MacOS 10.4.6 y más recientes

Desempeño Criptográfico

- Operaciones de llave 1024-bit y 2048-bit RSA
- Generación de llave con verificación de llave:
- Menos de 20 segundos para 1024-bit
- Menos de 90 segundos para 2048-bit
- Firma digital, menos de:
- .45 segundos para 1024-bit
- 1.23 segundos para 2048-bit

APIs Criptográficos

- PKCS #11
- Microsoft Crypto API
- Microsoft PC/SC
- Apple Native PC/SC

Algoritmos Criptográficos

Llave Asimétrica

- RSA 1024-2048-BIT
- Diffie-Hellman

Llave Simétrica

- 3DES
- AES 128, 192, 256

Hash Digest

- SHA-1

Soporte opcional adicional para algoritmos

Características Físicas

Hardware

- Memoria 64K

Conectividad

- USB 1.1/2.0 en cumplimiento
- 1.5 Mbits transferencia por segundo

Estandáres Regulatorios

- FCC Part 15 – Clase B
- CE



Corporate Headquarters: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524, Email: info@safenet-inc.com

EMEA Headquarters: Tel.: + 44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters: Tel: + 852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

www.safenet-inc.com